Software Engineering Challenges for Investigating Cyber-Physical Incidents

Conference or Workshop Item

Software Engineering Challenges For Investigating Cyber-Physical Incidents

Faeq Alrimawi
Lero, the Irish Software Research Centre
Limerick, Ireland

Liliana Pasquale
University College Dublin & Lero, the Irish Software Research Centre
Dublin, Ireland

Bashar Nuseibeh
The Open University & Lero, the Irish Software Research Centre
UK / Ireland

Abstract— **Cyber-Physical Systems (CPS) are characterized by the interplay between digital and physical spaces. This characteristic has extended the attack surface that could be exploited by an offender to cause harm. An increasing number of cyber-physical incidents may occur depending on the configuration of the physical and digital spaces and their interplay. Traditional investigation processes are not adequate to investigate these incidents, as they may overlook the extended attack surface resulting from such interplay, leading to relevant evidence being missed and testing flawed hypotheses explaining the incidents. The software engineering research community can contribute to addressing this problem, by deploying existing formalisms to model digital and physical spaces, and using analysis techniques to reason about their interplay and evolution. In this paper, we use a motivating example to describe some emerging software engineering challenges to support investigations of cyber-physical incidents. We review and critique existing research proposed to address these challenges, and sketch an initial solution based on a meta-model to represent cyber-physical incidents and a representation of the topology of digital and physical spaces that supports reasoning about their interplay.**

Keywords-component; Digital Investigation; Cyber-Physical Systems; CPS; Incidents.

I. INTRODUCTION

Cyber-Physical Systems (CPS) integrate computation, communication, and physical processes for the purpose of creating systems that are more capable, collaborative, and autonomous [1]. Applications of CPS [2] can be found in various domains including industrial control, transportation, and healthcare systems. This integration enables the interplay between the digital and physical spaces as events happening in the digital space can have an impact in both the physical and digital spaces and vice-versa. For example, in a smart building, a rise in the measured temperature of a room will trigger a digital process to issue a command to an air conditioner to start cooling the room.

Incidents occurring in CPS are increasing in number and sophistication as such systems become more pervasive [3]. Many of these incidents have caused significant damage to both digital and physical assets. For example, in the Ukrainian power grid incident [4], computer networks of three energy distribution companies were exploited to reach devices that control electricity distribution, and subsequently disable them by using a malware. This incident caused a power outage for about 225,000 customers over several areas.

Digital investigation process is identified as the use of scientific methods for the purpose of preserving, collecting, validating, identifying, analyzing, interpreting, documenting, and presenting digital evidence obtained from various digital resources to facilitate criminal events reconstruction or to predict unauthorized events that can cause harm [5]. Traditional investigation processes may not be adequate to investigate cyber-physical incidents, as they may overlook the extended attack surface of CPS. In particular, as cyber-physical incidents have only emerged in recent years, investigators might not be able to rely on their previous experience to explain how incidents have occurred. Moreover, investigative software tools are not developed with the aim to collect and analyze evidence related to incidents exploiting the interplay between digital and physical spaces (hereafter referred as interplay). As a consequence, investigators are prone to overlooking relevant evidence and may formulate flawed hypotheses explaining the incident.

In this paper, we argue that the activities performed during investigations of cyber-physical incidents should be driven by the interplay that the target CPS inhabits. To achieve this aim, we envision a solution building on existing research proposed within the software engineering community. In particular, modeling formalisms [6] have been developed to represent digital and physical spaces, and also analysis techniques [7] have been applied to reason about their interplay and evolution. In this paper, we use a motivating example of a cyber-physical incident to motivate our problem and describe the software engineering challenges to support investigations of such incidents. We also review some of the relevant literature that has been proposed to address these challenges. Moreover, we sketch an initial solution based on a meta-model to represent cyber-physical incidents and a representation of the topology of digital and physical spaces to reason about their interplay. Both representations will potentially enable reasoning about how cyber-physical incidents can occur and thus support some of the activities of an investigation.

978-1-5386-4043-2/17 $31.00 © 2017 IEEE
DOI 10.1109/SEsCPS.2017.9

The rest of the paper is organized as follows. Section 2 describes our motivating example. Section 3 discusses the software engineering challenges and their corresponding related research. Section 4 describes our initial solution and Section 5 concludes the paper.

II. MOTIVATING EXAMPLE

We motivate the problem of traditional investigations of cyber-physical incidents by presenting an incident scenario that could take place in a smart building. Fig. 1 represents the physical and digital spaces in which the incident can occur as well as the steps of the incident scenario.

As shown at the bottom of Fig. 1, the physical space is the 2nd floor plan of a research center. The floor plan is composed of a *server room* containing *servers* storing sensitive information (e.g., secret formulas), an *HVAC* (Heating, Ventilation, and Air Conditioning), and a *fire detector*. The floor also has a *toilet* containing *smart lighting* devices, and a *control room* containing a *workstation* through which building administrators can monitor and configure the operations of the devices through the IP network. The HVAC, the fire detector and the lighting devices are from the same vendor are connected to an installation bus adopting the KNX protocol [8]. The installation bus allows the devices to communicate between themselves, and also to send data (e.g., temperature) through the bus network to control processes (lighting, temperature, and alarm) running elsewhere. These processes use the received data to determine the status of the system, and issue commands to the physical devices to control certain properties of the environment (e.g., adjust the temperature). Data received by the control processes as well as the commands they issue are stored securely in a database and can be accessed by the building administrators through the workstation.

As shown at the top of Fig. 1, the digital space of the smart building is composed of the control processes (temperature, alarm, and lighting), the database in which sensor data are stored, and the IP and Bus networks.

In our example, the offender is a visitor who causes the incident by performing the following steps. 1) The visitor reaches the research floor and goes to the toilet. 2) She then connects her laptop to the installation bus (e.g., by exploiting proximity to the smart lights). 3) Subsequently, she collects data transmitted over the bus, and uses it to identify the devices in the floor through their physical source address, which is a 16-bit field containing information about the area, line, and device numbers. 4) She locates the devices in the server room by analyzing collected data. 5) The offender then sends special malware to the devices in the server room. This malware exploits vulnerabilities, such as those present in Trane HVACs [9], to compromise and disable the HVAC and the fire detector. 6) Simultaneously, the offender sends tampered temperature measurement data to the temperature control process on behalf of the fire detector and the HVAC in order to hide the temperature increase in the server room. Finally, the servers heat up, damaging or losing the information they store.

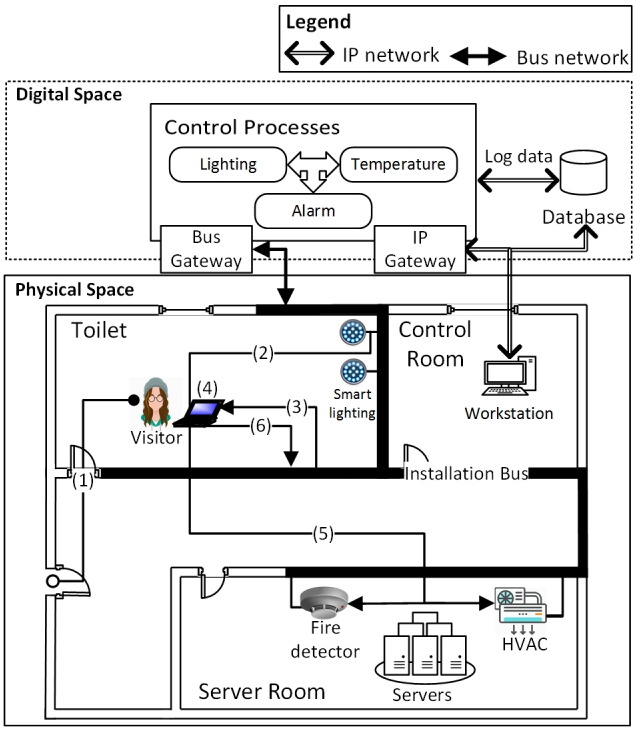

Figure 1. Digital and physical spaces of a smart building in which our incident example can take place.

Offenders can exploit the interplay in other ways. For example, an offender can get access to the IP network and send emails containing malware to employees. The malware can be embedded within a Microsoft Office document, and can exploit the macro functionality to install itself on the target machine, similarly to what happened in the Ukrainian incident [4]. The malware can subsequently compromise the smart devices that are controlled by the compromised target machine.

The interplay in the smart building has *extended the attack surface*. The physical reachability to the floor, the physical connectivity to the installation bus, and lack of security measures (e.g., encryption of transmitted data) in the KNX protocol gave the offender digital accessibility to the HVAC. Additionally, the interplay allows the propagation of an incident's impact from one component to others (cascaded impact). For example, the malware compromised the HVAC and the fire detector leading to a raise in the server room's temperature, consequently damaging the servers. The interplay enabled new and unusual interactions between different digital and physical components in the smart building (e.g., physical damage to the servers is caused through digital connectivity to the installation bus). Thus, investigators may overlook these interactions and consequently ignore relevant evidence such as transmission delays of KNX traffic between the smart light in the toilet and the lighting control process. Moreover, some data might not be available for examination because it is only stored in volatile memory (traffic transmitted over bus network) or might be tampered with by an offender. Hence this data might be lost if not preserved proactively. As a consequence,

an investigation can reach flawed conclusions. For example, the investigators may hypothesize that the servers were damaged due to a hardware failure, since they did not find any evidence indicating the occurrence of a physical incident (e.g., break and entry into the server room) or a cyber incident (e.g., a malware was installed in the server).

III. RESEARCH CHALLENGES

To address the problems described in the previous section it is necessary to provide awareness of how an incident can take place in a CPS, particularly how it can exploit the interplay. Thus analysis techniques should be applied on the representation of CPS to reason about how the interplay can be exploited by an offender to cause an incident. Analysis techniques can also help investigators to support event reconstruction in order to formulate and test robust incident hypotheses. Moreover, a system should be "ready" before an investigation of an incident is needed. This is referred to as forensic readiness that is the capability of a system to be prepared for future incident investigations by proactively collecting and storing potential evidence in a way that can maximize its use, while minimizing the costs of an investigation [10]. However, to date, only general organizational guidelines have been provided to achieve forensic readiness. Little or no attention has been given to how forensic-ready software systems can be designed systematically.

We now identify some software engineering challenges related to i) representing CPS and cyber-physical incidents and reasoning about how incidents can occur; ii) event reconstruction and iii) forensic-readiness requirements. For each challenge we also review existing related research and provide an illustration of the challenge with reference to our motivating example. The last subsection focuses on specific challenges related to engineering CPS that are forensic-ready.

A. Representing and Reasoning About CPS & Incidents

Representing CPS requires explicitly representing the interplay between digital and physical spaces. To achieve this aim, it is necessary to represent the main elements composing a CPS, their relationships and dynamics. Elements composing a CPS could be physical devices (e.g., HVAC, laptops), locations (e.g., the server room), digital processes (e.g., temperature control process), and agents. Relationships between these elements might be related to physical containment (e.g., the server room contains the HVAC) or digital containment (e.g., the temperature control process is executing on a server). Other relationships might be related to physical connectivity (e.g., a room is connected to another through a door) or digital connectivity (e.g., a laptop is connected to the installation bus). Dynamics are changes in the relationships between the elements caused by the execution of actions by agents. For example, the offender can establish physical connectivity between her laptop and the smart lights (e.g., she connects a microcontroller device to the smart lights). Explicit representation of the interplay can facilitate reasoning aimed to answer investigative questions, such as "how was the offender able to reach the HVAC?". In our example, an adequate representation of the interplay could help identify physical connectivity between smart lights and HVAC devices through the installation bus as a possible path to reach the HVAC. However, the difficulty lies in identifying spatial relationships (e.g., containment, connectivity) among elements and their dynamics, since CPS are a fairly new application domain providing emergent interactions between their components.

Pasquale et al. [11] have suggested that an explicit representation of the interplay of both digital and physical spaces can be used to engineer adaptive security systems. They propose *topology* as a key aspect to represent various spatial relationships such as containment and proximity. In a more recent work, Tsigkanos et al. [12] propose the use of Bigraphical Reactive Systems (BRS) to represent the topology. They apply model checking to reason about how the evolution of such topological relationships could determine security threats at runtime. This work could be used to identify potential digital evidence at runtime. This can be accomplished by identifying the elements of a CPS involved in the evolution of a topological configuration leading to an incident and their interactions.

Identification of an incident from the analysis of the CPS dynamics is likely to be intractable. This is due to the many different ways in which the elements composing a CPS and their relationships can evolve. Therefore, a representation of the CPS should be complemented with a high-level representation of the actions characterizing incidents and the involved elements (e.g., targeted assets, resources, offenders) of a CPS. The model should be general enough to allow application of the represented actions to different CPS. In our example, we could consider the incident represented as:

> *reach floor of targeted element => connect to installation bus through smart device => locate HVAC co-located with target device => compromise HVAC*

However, the challenge is to identify the common actions, elements, and relationships, which can be represented in an abstract way and applied to different situations. Moreover, producing a catalog of high-level incidents for CPS is challenging because knowledge regarding how cyber-physical incidents occur and their consequences is scarce [13]. Existing resources are developed and used for investigating primarily the digital space. Wood et al. [14] developed forensic datasets for educational purposes that include different scenarios involving different digital devices (e.g., mobile phones), which resemble real incident cases. However, the datasets include only activities performed on digital devices.

B. Event Reconstruction

Event reconstruction refers to the identification of the sequence of events that led to an incident [15]. In this phase, hypotheses regarding what happened are developed based on collected evidence.

A challenge for event reconstruction is cross-correlating collected evidence i.e. linkability. In CPS, physical processes operate in continuous time and space, while computational

processes operate in discrete time and space. In our example, temperature adjusting process in the server room operates in continuous time and space, while data generation and logging is done in discrete time and space. Thus, techniques for event reconstruction should take into account the different types of events (digital and physical) and their properties. Another challenge is the generation of large number of plausible hypotheses. This is due to the interplay in CPS and extended attack surface, which means that one event can be caused by potentially many elements (computational, communication, or physical). Thus, efficient, accurate, and precise event reconstruction approaches are required to minimize the number of generated hypotheses to relevant-plausible ones.

Gladyshev and Patel [16] propose a finite state machine (FSM) approach to formalize hypothesis generation of an incident in digital investigations. Formalization is done through defining the event reconstruction problem as finding all possible explanations for a given evidential statement with respect to the FSM. James et al. [17] try to address the state explosion problem by converting the FSM into deterministic FSM which reduces the size of the state machine. However, it is still a problem for real incidents where many complex events take place, thus, it is not applicable for such cases. Khan et al. [18] propose the use of artificial neural networks to handle large data generated in an incident to reconstruct the timeline of events. A limitation of this work is admissibility of results, since some parameters used in the learning step are unknown, as stated by the authors.

C. *Forensic Readiness Requirements*

Forensic readiness is particularly important for CPS because some of the data produced by the devices composing a CPS might be volatile or tampered with. This might depend on the fact that some devices are resource-constrained, might be shut down, or lack security measures. For example, temperature sensors have limited resources; hence, data generated by them are kept for a short period and then deleted from the devices. So, in our example, the investigators might not be able to know the temperature before or during the incident if temperature measurements were not collected proactively. Thus, investigators would not be able to support or refute the hypothesis that the rise in the room's temperature was the cause of the servers' failure. In addition, offenders might tamper with generated data to hide their traces and/or mislead investigations. In our example, the offender tampered with the temperature data sent to control processes to hide any increase in the temperature. Consequently, misleading investigators to believe that the servers were damaged because of a hardware failure.

To support forensic readiness, it is necessary to explicitly elicit and manage forensic readiness requirements. Some of these requirements prescribe to collect and store data representing the occurrence of events related to offender's actions performed during potential incidents. Eliciting forensic readiness requirements is challenging because the unusual interactions between events in both the digital and physical spaces make it difficult to identify data to be collected proactively. For our example, this data could be control commands issued to the HVAC through the installation bus, and/or temperature measurements in the server room.

Forensic readiness requirements also need to be traded off with other requirements. In particular, high availability requirement of the HVAC suggests that evidence collection and storage activities should be minimally intrusive and be performed while the device is operating, because it cannot be shut down. Moreover, CPS can generate large and heterogeneous data. Therefore, preserving any data produced by the CPS devices is infeasible due to the long time that such data will require to be analyzed during an investigation.

Pasquale et al. [19] propose an evidence collection approach aimed to adaptively identify relevant evidence that should be collected proactively by IaaS (Infrastructure as a Service) cloud service providers. This evidence is identified from potential attack scenarios that may exploit well known vulnerabilities, such as those documented in the Common Vulnerabilities Exposures CVE dictionary. However, the focus of the work is on the digital space and digital investigations, and therefore does not consider the interplay between the physical and digital spaces.

Taylor et al. [20] propose a general process for eliciting forensic readiness requirements from forensic policies. Such polices specify what events and related data need to be managed. Forensics policies are identified by selecting the digital assets to be protected, performing risk assessment, excluding unworthy assets for prosecution, and identifying related data. However, this approach is not automated. Furthermore, it is not tailored to incidents occurring in CPS as it does not consider events determined by the interplay between cyber and physical spaces.

The requirements engineering community has demonstrated an increasing interest [21] in supporting incidents investigations. For example, in the context of social media incident investigations, Tun et al. [22] identify three main requirements related to evidence collection: maintaining privacy, continuity, and integrity of digital evidence. Similarly, Gray et al. [23] have proposed a technique to assess risks that local password managers can bring when maintaining integrity and authenticity of passwords. This technique could be applied to other sources of evidence to ensure integrity and authenticity of the data preserved proactively. However, none of this work has proposed a framework to elicit forensic readiness requirements nor has addressed the implementation of such requirements in cyber-physical systems.

IV. TOWARDS A SOLUTION

In this paper we begin to support engineering forensic-ready cyber-physical systems by suggesting a systematic approach to elicit and manage forensic readiness requirements. In particular, our approach supports the identification of what evidence should be collected and when, which may also help investigators formulate incident hypotheses and perform event reconstruction. Our solution builds on two key modeling activities: i) modeling cyber-physical incidents and ii) modeling the CPS in which these

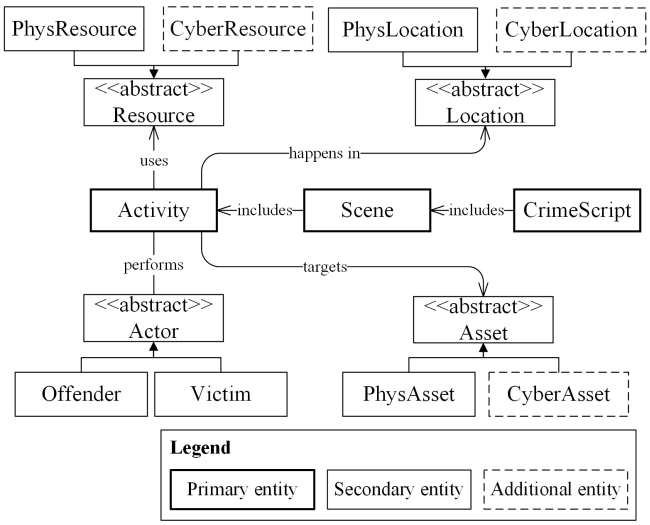

Figure 2. Simplified version of the meta-model of cyber-physical incidents.

incidents can occur, including the interplay between CPS elements.

Modeling cyber-physical incidents requires representing the activities performed by the victim and the offender(s), as well as other concepts such as location, which might better specify the incident activities. A simplified version of the meta-model representing cyber-physical incidents is shown in Fig. 2. This version does not include entities and attributes, such as crime motives and goals, because they are not fundamental to describe our solution. The meta-model was implemented as an Eclipse plugin publicly available[1].

To achieve this aim, first we build on the concept of "Crime Script" [24]. This is widely used in criminology to describe the sequence of activities of a physical incident, such as subway mugging. In particular, we extracted *primary*, *secondary* and *additional entities*. Primary entities are those represented in all crime script models published in the literature. Examples of primary entities are the *crime script* itself. This *includes* a set of *scenes*, which are the settings in which certain activities take place (e.g., preparation scene). Each scene in turn *includes* a set of *activities* an agent performs during the incident. Secondary entities are those mentioned - implicitly or explicitly - in most of the models published in the literature [25][26]. These are used to relate an activity to the agent performing it (victim or offender). Additional entities and relationships are those we included in our meta-model to represent domain-specific entities of cyber-physical incidents, such as *actor*s, *asset*s, *resource*s and *location*s. These entities are abstract and can be extended by specific entities represented in the model of the CPS, such as specific digital (HVAC software) and physical locations (e.g., the server room) and assets.

In the meta-model, *an asset* is an entity that can be harmed in an incident. *Cyber asset* can be any data that is stored on an electronic device or being transmitted over a network. *Physical asset* is a physical entity such as a server. A *location* represents a place where an activity or a sequence

[1]tinyurl.com/h2qr87x

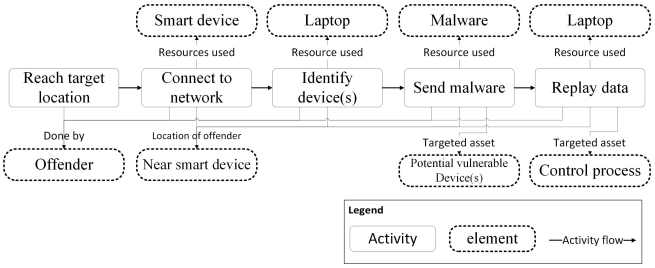

Figure 3. Partial incident template based on the meta-model.

of activities of a scene is performed. *Physical location* is a real world location (e.g., a room) where an activity or a sequence of activities of a scene takes place. *Cyber location* represents a place in the cyber space such as an IP address, a forum, or a folder in a computer. An *actor* represents an individual who performs an activity, and can be the *offender* or the *victim*. A resource represents a tool needed to perform an activity. *Physical resource* refers to physical tool used by an offender in an incident (e.g., laptop). *Cyber resource* represents software tools that an offender can use to assist them in an incident (e.g., malware).

The meta-model has the potential to provide a systematic and rich representation of cyber-physical incidents, since it encompasses not only the activities of an incident but also related elements and relationships in the digital and physical spaces (e.g., location, assets, and actors), that were underrepresented in the original use of the Crime Scripts.

Moreover, the possibility to extend abstract entities with domain-specific entities identified from the representation of the CPS makes our meta-model extensible and general enough to be applied to different types of CPS.

We aim to use the primary and the additional entities of the crime-script meta-model to instantiate general incident templates providing a high-level, domain independent representation of a cyber-physical incident. An incident template for our example is shown in Fig. 3. We subsequently aim to plug concrete domain-dependent entities depending on the specific cyber-physical system of interest to identify whether an incident is feasible in a specific CPS and - if so - how it can occur.

We also suggest the explicit representation of CPS topology and its dynamics in order to model the interplay. Topology refers to the *spatial relationships among elements,* which include *containment* and *connectivity*. We propose such an explicit representation and reasoning about the topology of a CPS, since it provides a way to better understand the cause-effect relationships between different elements in the digital and physical spaces. In our example, the topology of the digital and physical spaces can be represented as shown in Fig. 4. The floor *contains* server room, toilet, and control room. Server room *contains* servers, HVAC, and fire detector. The toilet *contains* smart lights. Control room *contains* workstation. The HVAC, fire detector and smart lights are *physically connected* to each other through the installation bus. The HVAC, fire detector and smart lights are *digitally connected* to each other and to control processes through the bus network. The Workstation

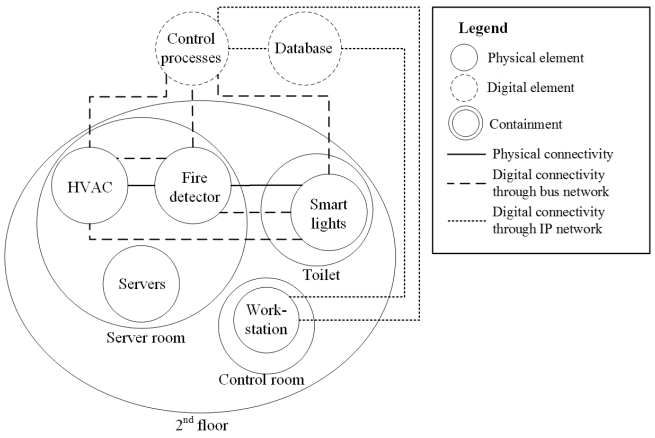

Figure 4. Topology representation of the digital and physical spaces in the motivating example.

is *digitally connected* to the control processes and database through the IP network.

The topology representation in Fig. 4 can be reasoned about to answer questions such as "how was the offender able to reach the HVAC?". The answer to this question would be all possible paths that the analysis of the topology can find. For example, it finds the following paths:

Path 1: *enter floor => enter server room => physically reach the HVAC*
Path 2: *enter floor => enter control room => connect digitally to control processes using the workstation => digitally reach the HVAC through control processes*
Path 3: *enter floor => enter toilet => physically connect to smart lights => digitally reach HVAC through bus network*

The analysis of the full topology of a CPS could potentially return a large number of possible paths, since, as we explained in section III.A, there are many different ways in which the elements composing a CPS can interact. However, not all paths found have the same significance. Some paths might not lead to an incident, so, there is no need to analyze them. Some paths might have a very low probability of being exploited; hence, they should be given a lower priority. There might only be part of the paths that require close analysis. Therefore, in order to identify which paths are more important, we need to generate concrete cyber-physical incident instances. These incident instances can be used to identify which cyber-physical paths have higher probability of being exploited than others. For example, the incident template shown in Fig. 3 and the topology representation in Fig. 4 can be used to produce the partial incident instance shown in Fig. 5.

Analyzing this incident and the three generated paths would provide information that path 3 is the path that the offender most likely exploited (or might exploit), in this case, since path 3 and the incident instance identify more common elements (e.g., toilet, smart lights).

We intend to use the meta-model to build cyber-physical incident templates. Moreover, we intend to use appropriate modeling formalisms [6] to model the CPS topology and its dynamics. We will use the model of the topology and the incident templates to support forensic readiness and event

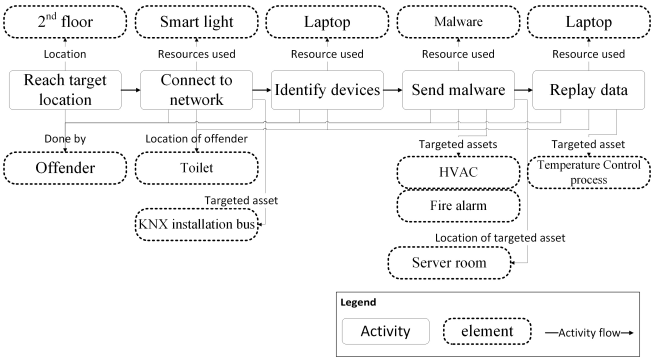

Figure 5. Partial incident instance.

reconstruction activities. In forensic readiness, we plan to develop analysis techniques that generate potential incident instances. Incident instances can be used to identify potential digital evidence by extracting relevant elements such as targeted assets, and location. For example, we can analyze the partial incident instance shown in Fig. 5 to extract elements such as the *smart light* and *KNX installation bus*. These might constitute potential evidence sources from which data should be proactively collected. Additionally, *when* to start collecting data can be identified incident instances. For example, collecting data from the *KNX installation bus* can start when a device is connected to the bus, or when one of the connected devices (e.g., the smart light) becomes offline.

In event reconstruction, we intend to develop analysis techniques that reason about the representation of the topology, potential incident instances, and collected evidence about the incident, to generate closely-relevant and plausible hypotheses about what happened. Generated hypotheses can help identify evidence that can support or refute them by extracting information from the incident instances such as resources used. For example, in the partial incident instance shown in Fig. 5, combining the elements *toilet* and *smart light* can provide investigators with clues on *where* and *what* to look for to extract evidence.

It is worth mentioning that incomplete information and uncertainty in incident templates and instances are expected. On the one hand, it might be the case that the incident templates created do not contain all possible activities that can lead to an incident. So, continuous updating of the templates is required to include any missing activities that are discovered from investigating various incidents. On the other hand, an activity in an incident template can be interpreted in various ways by incident instances, or it can have no interpretations. Therefore, we will explore ways to assess the likelihood of different interpretations of an incident activity and the reasons why an activity cannot be performed in the cyber-physical space.

V. CONCLUSION AND FUTURE WORK

In this paper we argued that cyber-physical incidents should be investigated differently from traditional investigations. This is due to the interplay between digital and physical spaces that CPS inhabit, and the consequent extended attack surface. We discussed software engineering

challenges in relation to the interplay in CPS. These challenges include the representation and reasoning about the interplay and incidents, event reconstruction and forensic readiness requirements. We proposed two potential modeling components of a solution to support investigations of cyber-physical incidents: a meta-model to represent cyber-physical incidents and the explicit representation of topology. These could be used in the forensic readiness phase to identify potential incidents, and subsequently potential evidence to collect. Moreover, they could be used in the event reconstruction phase to generate hypotheses about what happened, and what evidence could support/refute these hypotheses.

In future work, we intend to identify suitable modeling formalisms to represent the topology of digital and physical spaces and their dynamics. We also need to develop analysis techniques that take advantage of the meta-model and topology representation to support forensic readiness and event reconstruction phases. Finally, we need to evaluate our work by creating prognostic and diagnostic scenarios to test our techniques, and then consider ways of obtaining some metrics such as error rates for identifying potential incidents and error rates for generated hypotheses.

ACKNOWLEDGMENT

This work was partially supported by ERC Advanced Grant no. 291652 (ASAP) and Science Foundation Ireland grants 10/CE/I1855, 13/RC/2094 and 15/SIRG/3501.

REFERENCES

[1] E. A. Lee, "CPS foundations," in *Proceedings of the 47th Design Automation Conference*, 2010, pp. 737–742.

[2] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4242–4268, 2014.

[3] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann, 2015.

[4] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016.

[5] G. Palmer, "A road map for digital forensic research," *First Digit. Forensic Res. Work.*, 2001.

[6] R. Milner, "Bigraphical Reactive Systems," *CONCUR 2001 --- Concurr. Theory*, vol. 2154, pp. 16–35, 2001.

[7] G. Perrone, S. Debois, and T. T. Hildebrandt, "A Model Checker for Bigraphs," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 2012, pp. 1320–1325.

[8] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication Systems for Building Automation and Control," *IEEE*, vol. 93, no. 6, pp. 1178–1203, 2005.

[9] Krebs on Security, "IoT Reality: Smart Devices, Dumb Defaults," 2016. [Online]. Available: https://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/. [Accessed: 18-Feb-2017].

[10] R. Rowlingson, "A ten step process for forensic readiness," *Int. J. Digit. Evid.*, vol. 2, no. 3, pp. 1–28, 2004.

[11] L. Pasquale, C. Ghezzi, C. Menghi, and C. Tsigkanos, "Topology aware adaptive security," in *Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, 2014, pp. 43–48.

[12] C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh, "On the Interplay Between Cyber and Physical Spaces for Adaptive Security," *IEEE Trans. Dependable Secur. Comput.*, 2016.

[13] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems," in *Workshop on future directions in cyber-physical systems security*, 2009, p. 5.

[14] K. Woods, C. A. Lee, S. Garfinkel, D. Dittrich, A. Russell, and K. Kearton, "Creating realistic corpora for security and forensic education," in *Proceedings of the Conference on Digital Forensics, Security and Law*, 2011, pp. 123–134.

[15] S. Jeyaraman and M. J. Atallah, "An empirical study of automatic event reconstruction systems," *Digit. Investig.*, vol. 3, no. SUPPL., pp. 108–115, Sep. 2006.

[16] P. Gladyshev and A. Patel, "Finite state machine approach to digital event reconstruction," *Digit. Investig.*, vol. 1, no. 2, pp. 130–149, 2004.

[17] J. James, P. Gladyshev, M. T. Abdullah, and Y. Zhu, "Analysis of evidence using formal event reconstruction," in *Digital Forensics and Cyber Crime*, Springer, 2010, pp. 85–98.

[18] M. N. A. Khan, C. R. Chatwin, and R. C. D. Young, "A framework for post-event timeline reconstruction using neural networks," *Digit. Investig.*, vol. 4, no. 3–4, pp. 146–157, 2007.

[19] L. Pasquale, S. Hanvey, M. Mcgloin, and B. Nuseibeh, "Adaptive evidence collection in the cloud using attack scenarios," *Comput. Secur.*, vol. 59, pp. 236–254, 2016.

[20] C. Taylor, B. Endicott-Popovsky, and D. A. Frincke, "Specifying digital forensics: A forensics policy approach," *Digit. Investig.*, vol. 4, pp. 101–104, 2007.

[21] D. Alrajeh and L. Pasquale, "Welcome to the First Workshop on Requirements Engineering for Investigating and Countering Crimes (iRENIC 2016)," in *Requirements Engineering Conference Workshops (REW)*, 2016, p. 92–i.

[22] T. Tun, B. Price, A. Bandara, Y. Yu, and B. Nuseibeh, "Verifiable Limited Disclosure : Reporting and Handling Digital Evidence in Police Investigations," in *Requirements Engineering Conference Workshops (REW)*, 2016.

[23] J. Gray and V. N. L. Franqueira, "Forensically-Sound Analysis of Security Risks of using Local Password Managers," in *Requirements Engineering Conference Workshops (REW)*, 2016, pp. 114–121.

[24] D. Cornish, "Crimes as scripts," in *Proceedings of the international seminar on environmental criminology and crime analysis*, 1994, pp. 30–45.

[25] H. Brayley, E. Cockbain, and G. Laycock, "The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking," *Policing*, vol. 5, no. 2, pp. 132–143, 2011.

[26] D. Cornish, "The procedural analysis of offending and its relevance for situational prevention," *Crime Prev. Stud.*, vol. 3, pp. 151–196, 1994.